**Suricata - Security #3168**

tls: out of bounds read

09/17/2019 09:47 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Target version:</td>
<td>4.1.5</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>Git IDs: b32b4642212dac764ca67a5fce8c97394 e199631</td>
</tr>
<tr>
<td>CVE:</td>
<td>2019-1569</td>
</tr>
</tbody>
</table>

**Description**

```
==7789==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000031d6 at pc 0x555555dec3b7 bp 0x7fffffff8530 sp 0x7fffffff8528
READ of size 1 at 0x6060000031d6 thread T0
#0 0x555555dec3b6 in TLSDecodeHSHelloExtensionSupportedVersions /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:962:42
#1 0x555555de8b1b in TLSDecodeHSHelloExtensions /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1224:23
#2 0x555555de33d3 in TLSDecodeHandshakeHello /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1353:11
#3 0x555555d4d4eb in SSLv3ParseHandshakeType /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c
#4 0x555555d4d903c in SSLv3ParseHandshakeProtocol /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1620:14
#5 0x555555dcb3b2 in SSLv3Decode /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:2293:22
#6 0x555555d3402 in SSLDecode /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:2471:30
#7 0x555555d741f6 in AppLayerParserParse /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-parser.c:1188:13
#8 0x555555d40898 in LLVMFuzzerTestOneInput /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f832)
#9 0x5555556ce3832 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f832)
#10 0x5555556d3da4 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f832)
#11 0x5555556cdecace in fuzzer::FuzzerDriver(int*, char***, int (*) (unsigned char const*, unsigned long)) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x177fda4)
#12 0x5555555c23d23 in main (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x1788ace)
#13 0x7fffffff6c8e2 in __libc_start_main (/usr/lib/libc.so.6+0x26ee2)
#14 0x5555555c23edd in _start (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x6cfedd)
```

**Related issues:**

Copied to Security #3169: tls: out of bounds read (5.x) - Closed

**History**

- #1 - 09/17/2019 09:47 AM - Victor Julien
  - Copied to Security #3169: tls: out of bounds read (5.x) added

- #2 - 09/24/2019 02:54 PM - Victor Julien
  - Status changed from Assigned to Closed
  - Priority changed from High to Normal

09/09/2020
- Private changed from Yes to No

https://github.com/OJSF/suricata/commit/b32b4642212dac75e67a5fcb8c97394e199631

#3 - 09/01/2020 09:06 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2019-15699
- Git IDs updated